Redes de Acesso

Parte B – Protocolos de Acesso

Mário Serafim Nunes

IST, Março 2006

1 Introdução

Os acessos à Internet têm vindo a crescer a forte ritmo, quer em número de utilizadores quer em tráfego gerado. As redes mais utilizadas para esses acessos são ainda a rede telefónica comutada (PSTN) e a RDIS, tendo contudo nos últimos anos sido desenvolvidas várias tecnologias ditas de "banda larga", com maiores débitos, de que se destacam nomeadamente em Portugal a ADSL e o HFC (*Hybrid Fibre Coax*).

Na Figura 1 apresenta-se um diagrama de acesso à Internet usando diferentes tecnologias e redes, nomeadamente através de PSTN, RDIS e ADSL.

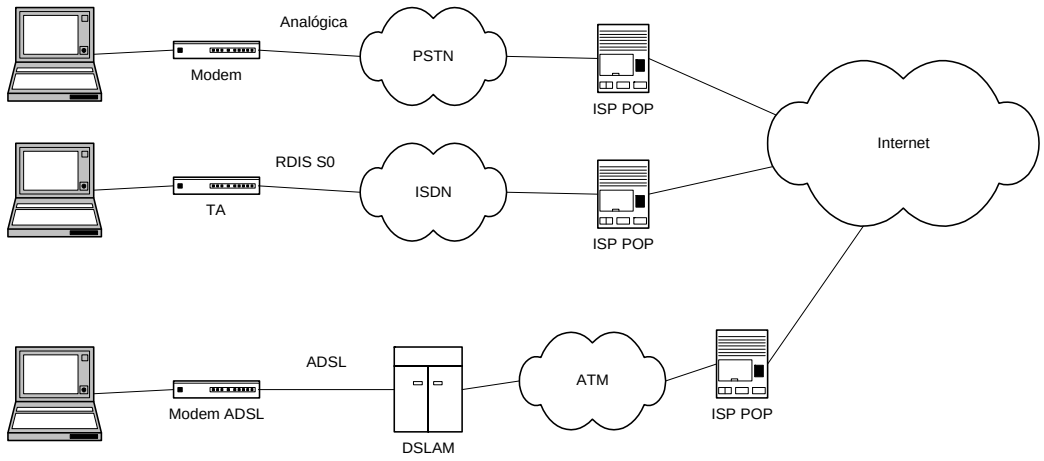

Figura 1 – Acessos à Internet

Apesar de as tecnologias e redes de acesso serem diversas, a grande maioria utiliza como protocolo de acesso o protocolo PPP (*Point-To-Point-Protocol*) do IETF (*Internet Engineering Task Force*).

Na Figura 2 apresenta-se o diagrama de protocolos no acesso através da rede telefónica PSTN, verificando-se que o protocolo PPP corresponde à camada 2 do modelo OSI.

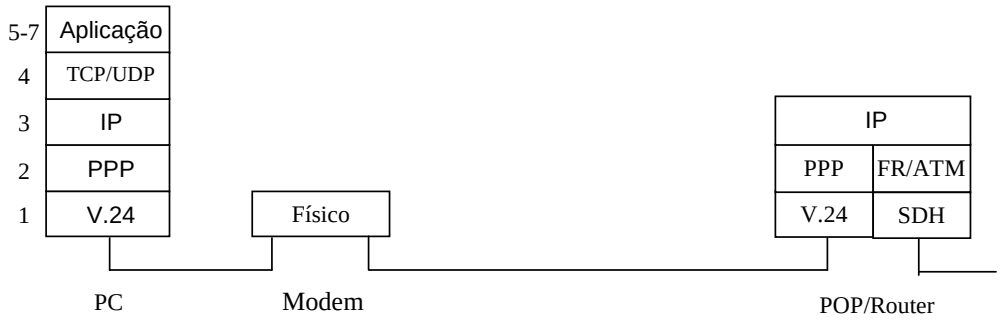

Figura 2 – Diagrama de protocolos no acesso à Internet através de PSTN

Na Figura 3 apresenta-se o diagrama de protocolos utilizado no acesso à Internet através de canal B de RDIS, onde se mostra apenas o plano de dados.

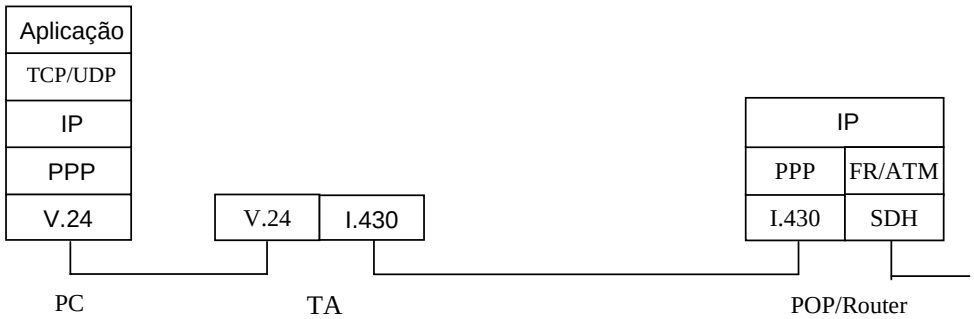

Figura 3 – Diagrama de protocolos de dados de acesso à Internet através de RDIS, canal B

Como o protocolo PPP baseado no protocolo HDLC (*High-level Data Link Control*), é oportuno listar os protocolos de ligação de dados baseados em HDLC actualmente definidos. Como se observa na tabela, os protocolos derivados de HDLC estão presentes em todas as modernas redes de comunicações, públicas e privadas, fixas e móveis.

Tabela 1 – Família de protocolos de ligação de dados baseados em HDLC

Nome	**Rede/norma**	**Descrição**
SDLC	*SNA (IBM)*	*Synchronous Data Link Control*
HDLC	Linha Série	High level Data Link Control
LLC	LAN	Logical Link Control
LAPB	X.25	Link Access Procedure, Balanced
LAPD	ISDN	Link Access Procedure for D Channel
LAPDm	GSM	LAPD for Mobile Links
LAPM	V.42	Link Access Procedure for Modems
LAPF	FR	LAP for Frame Relay
V.120	TA ISDN	ISDN Statistical Multiplexing
MTP-2	SS7	Message Transfer Part
PPP	Internet	Point-to-Point Protocol

2 Protocolos PPP

O protocolo PPP foi especificado pelo IETF inicialmente no RFC 1331 e posteriormente actualizado no RFC 1548 e no RFC 1661. Este protocolo providencia um método normalizado de transporte de datagramas multi-protocolo sobre circuitos ponto a ponto. O PPP suporta detecção de erros, múltiplos protocolos e negociação para atribuição de endereços IP na fase de conexão e autenticação.

O PPP é um protocolo que se situa na camada 2 do modelo de referência OSI, estruturado em tramas, apropriado para funcionar sobre Modems, linhas séries HDLC orientadas a octeto ou a bit, SONET/SDH e outras camadas físicas. Pode ser usado não só para ligações do tipo marcação em linhas telefónicas (*Dial-Up)* mas também para ligação entre *Routers* em linhas dedicadas.

O protocolo PPP é constituído por um conjunto de protocolos, sendo caracterizado por várias componentes:

1. Método de encapsulamento de dados em forma de trama que permite determinar o início e o fim de cada trama. Este formato também apresenta a vantagem de permitir a detecção de erros.
2. Um protocolo de ligação de dados LCP (*Link Control Protocol*), que permite iniciar a ligação, testar a qualidade da linha, negociar opções de configuração, como por exemplo o tipo de protocolo a ser usado nas fases seguintes, e finalmente interromper a ligação quando esta já não for necessária.
3. Um protocolo NCP (*Network Control Protocol*), que faz a multiplexagem de diferentes protocolos de nível superior (camada de rede), como por exemplo IP, IPX, AppleTalk, sobre a forma de negociação de opções de configuração.
4. Protocolos de autenticação (por exemplo CHAP ou PAP) para validação dos acessos dos utilizadores.

De acordo com a funcionalidade descrita, o protocolo PPP pode ser organizado em duas subcamadas, como se indica na Figura 4.

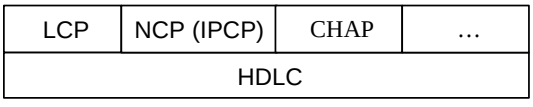

Figura 4 – Subcamadas do protocolo PPP

Para compreender como as várias componentes do PPP interagem, exemplifica-se uma situação real em que um utilizador em sua casa pretende contactar um *Internet Service Provider* (ISP) para se ligar temporariamente à Internet.

A primeira acção do PC cliente é fazer uma chamada ou um pedido de ligação através do *Modem* (Fase 1). Depois do *Modem* do lado do ISP responder e estabelecer a ligação física (Fase 2) e lógica (Fase 3) do canal, o PC cliente e o *Router* trocam pacotes do tipo LCP para a configuração da ligação (Fase 4). Terminado este estado os dados de autenticação opcionais são analisados pelo ISP (Fases 5) e em caso de sucesso é trocada uma série de pacotes NCP (IPCP no caso de se usar IP) (Fase 6) para configuração de parâmetros da camada de rede. Após este estado podem ser enviados dados (Fase 7).

Na Figura 5 exemplificam-se simplificadamente as diferentes fases de operação do PPP no acesso à Internet através da rede telefónica com Modem.

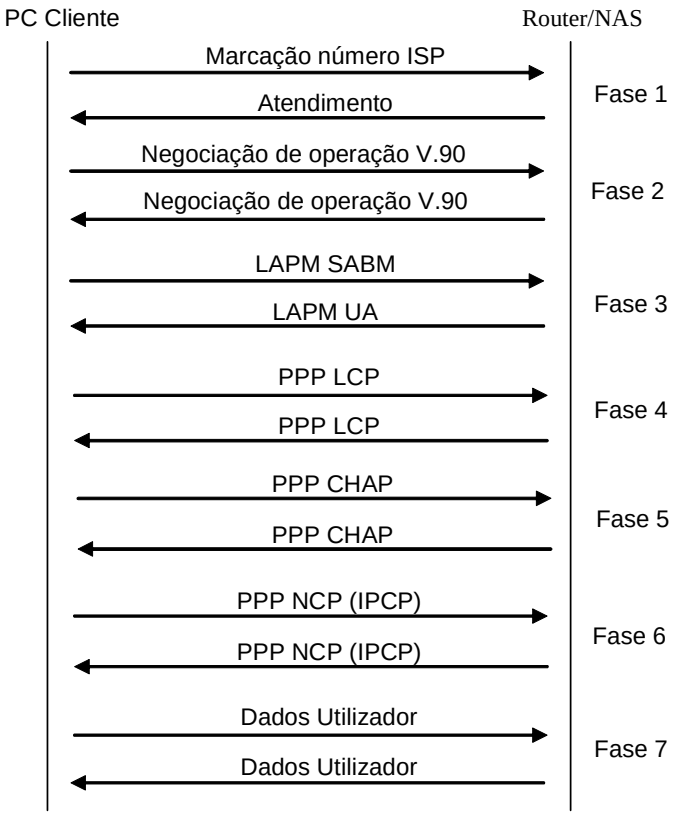

Figura 5 – Fases de operação de acesso à Internet com Modem e protocolo PPP

Uma das tarefas mais importantes da fase NCP é a atribuição dinâmica dos endereços de nível rede (IP no caso de IPCP) por parte do ISP, uma vez que estes são reduzidos e apenas são atribuídos durante a ligação para uso temporário. Uma vez terminada a ligação o *router* encarrega-se de libertar o endereço.

É na fase LCP que a sessão é encerrada ao nível da transmissão de dados, e de seguida o PC envia um sinal local de desconexão ao Modem para desligar a linha e libertar a camada física da conexão.

2.1 Formato de tramas PPP

A formatação dos pacotes PPP em HDLC é definida na RFC 1662, "PPP in HDLC-like Framing". Como se pode verificar na figura 6, o formato das tramas PPP em HDLC começa com um campo FLAG (7Eh), a que se seguem os campos *Address*, *Control*, *Protocol*, *Information*, FCS e FLAG.

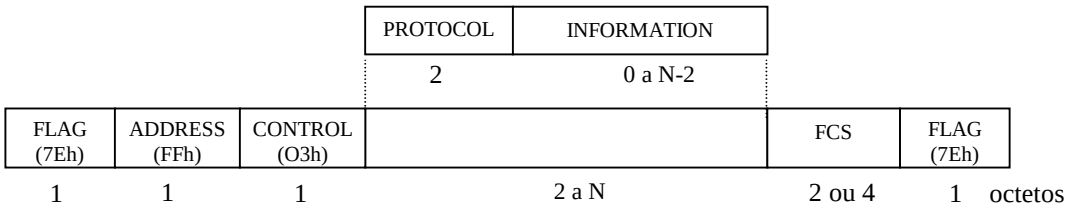

Figura 6 - Trama PPP

O campo **Address** tem o valor '11111111' (FFh), o que significa que a trama está orientada para todas as estações (*broadcast*). Os endereços, do tipo *broadcast* , devem ser sempre reconhecidos. Qualquer formato diferente de endereço deve ser acordado numa fase prévia de negociação. Campos de endereços não reconhecidos devem ser descartadas.

O campo **Control** ocupa um octeto e tem o valor '00000011' (03h), correspondente ao o comando UI (*Unnumbered Information*) com o bit P/F a zero, identificando a transmissão de dados em tramas não numeradas. Tramas com campos de controlo não reconhecidos devem ser descartadas.

O campo **Protocol** ocupa um octeto se for sujeito a compressão, ou dois octetos sem compressão, tendo como função identificar o conteúdo encapsulado no campo **Information** do pacote. A estrutura deste campo é especificada na recomendação ISO 3309, nomeadamente o mecanismo de extensão do campo de endereço.

Os valores do campo **Protocol** são definidos e actualizados pelo IANA (*Internet Assigned Number Authority*). A Tabela 2 mostra exemplos de alguns protocolos e os respectivos valores mais usados nas ligações PPP.

Tabela 2 – Valores do campo Protocolo de PPP

Valores (hex)	Protocolos
C021	LCP - Link Control Protocol
C023	PAP - Password-Authentication-Protocol
C025	LQR – Link Quality Report
C223	CHAP – Challenge Handshake Authentication Protocol
8021	IPCP – IP Control Protocol
80FD	CCP - Compression Control Protocol
0800	Dados IP

O campo **Information** é constituído por zero ou mais octetos, sendo constituído por dados correspondentes ao protocolo especificado no campo **Protocol,** onde o seu tamanho máximo é determinado pela negociação de opções do pacote LCP, por omissão 1500 Octetos**.**

O campo **FCS** (*Frame Check Sequence*) tem 16 bits por omissão mas por negociação poderá ocupar 32 bits. Trata-se de um campo de controlo calculado com base em todos campos da trama PPP excepto nos campos **Flag** e **FCS**.

2.2 Encapsulamento de dados PPP

Na RFC 1662 são definidos três tipos de formatos de encapsulamento de dados PPP em HDLC:

- HDLC Síncrono ao Bit
- HDLC Assíncrono (AHDLC)
- HDLC Síncrono ao Octeto

2.2.1 HDLC síncrono ao bit

O formato HDLC síncrono ao bit é o formato mais comum, sendo usado na maioria dos casos, em particular para débitos elevados.

Este formato corresponde ao HDLC padrão. Os pacotes PPP começam e terminam com um campo FLAG**,** que consiste numa sequência binária '01111110', 7Eh em hexadecimal. Este campo é um separador de tramas, portanto não deve existir uma sequência idêntica ao campo FLAG no interior da trama. É por isso usado "bit stuffing" (inserção de um bit zero após a ocorrência de 5 uns sucessivos) para manter a transparência da informação no interior das tramas.

2.2.2 HDLC assíncrono (AHDLC)

O HDLC assíncrono é usado em interfaces série de baixo débito, nomeadamente em Modems assíncronos e interfaces séries assíncronas, por exemplo portas série de PC. Neste formato são usados caracteres especiais para identificar funções, nomeadamente o carácter 7Eh para delimitação de trama e o carácter 7Dh para Escape. O carácter 7Eh marca o início e fim da trama HDLC, sendo também enviado entre tramas sucessivas. O carácter 7Dh permite usar os caracteres 00h-1Fh e 7Eh, os quais são antecedidos de 7Dh, sendo este mecanismo denominado "octet stuffing".

Para manter a transparência, cada carácter de dados com código igual à Flag (7Eh), ao Escape (7Dh) ou a um carácter de controlo definido no mapa ACCM (*Async Control Character Map*) é substituído por dois caracteres, o primeiro dos quais é um Escape e o segundo um octeto que é obtido através da operação "ou exclusivo" do octeto original com 20h, isto é, o octeto original com o 6º bit mais significativo complementado.

Na tabela 3 mostram-se alguns exemplos de codificação com "octet stuffing".

Tabela 3 – Exemplos de codificação com "octet stuffing"

Caracter	Valor (Hex)	Sequência codificada (Hex)
Flag	7e	7d 5e
Escape	7d	7d 5d
ETX	03	7d 23
XON	11	7d 31
XOFF	13	7d 33

Mostra-se em seguida uma sequência de início de pacote PPP sem e com "octet stuffing", em que se considera que os caracteres FF e 03 não são permitidos e em que o carácter inicial 7E é a flag de início da trama HDLC:

Pacote PPP sem "octet stuffing": 7E FF 03 C0 21 ...

Pacote PPP com "octet stuffing": 7E *7D* DF *7D* 23 C0 21 ...

2.2.3 HDLC síncrono ao octeto

O HDLC Síncrono ao octeto é usado em canais síncronos. É semelhante ao AHDLC excepto no facto de os caracteres de controlo não necessitarem de usar Escape ou "octet stuffing". Na RFC 1618, "PPP over ISDN" esta formatação é uma das opções consideradas no transporte de PPP em canais B de RDIS.

2.3 Diagrama de estados de PPP

As diferentes fases de processamento do protocolo podem ser descritas com base num diagrama de estados simplificado apresentado na Figura 7.

2.3.1 Estado Inactivo

A ligação começa e termina nesta fase. Quando há um evento externo (tal como a detecção de uma portadora no nível físico) indicando que a camada física está disponível para ser usada, o PPP prossegue para o estado de Estabelecimento da ligação.

Durante este estado a máquina de estados do LCP (descrito adiante), estará nos estados inicial ou *Starting*. Retorna-se ao estado Inactivo após a desconexão do Modem. Este estado torna-se muito curto nos casos de ligações *Hard-Wired (*por exemplo Modem Interno).

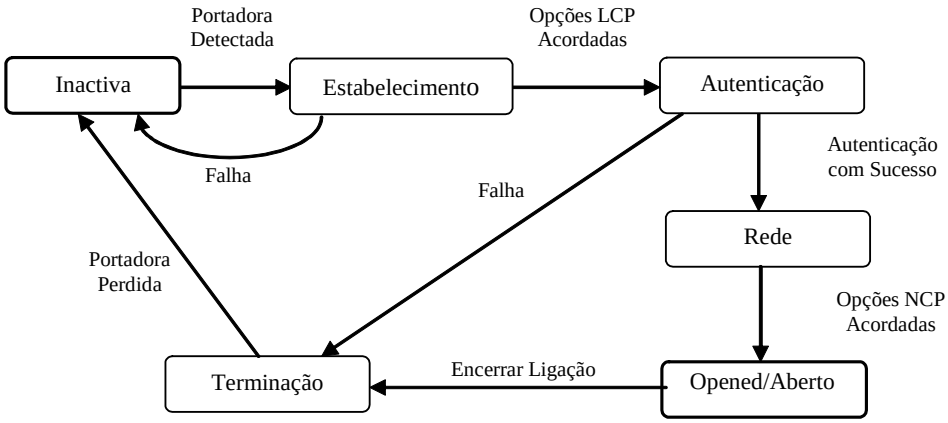

Figura 7 - Diagrama de estados de PPP

2.3.2 Estado de Estabelecimento

O protocolo de controlo da ligação (LCP) é usado para estabelecer a conexão mediante a troca de pacotes de configuração. O estado Aberto (*Opened)* é atingido depois da recepção e envio de pacotes *Configure-Ack* (descrito adiante). *Opened* é o último estado da máquina de estados da fase de estabelecimento.

Neste estado são negociadas as opções de configuração independentes do tipo de protocolos de rede a serem usados nas fases posteriores. A configuração de protocolos da camada de rede é feita por protocolos independentes (NCPs).

A recepção neste estado de pacotes que não sejam do tipo LCP devem ser descartados silenciosamente. A recepção de um pacote *Configure-Request* LCP nas fases seguintes resulta no retorno à reconfiguração da ligação.

2.3.3 Estado de Autenticação

Em algumas ligações a camada homóloga pode desejar que o utilizador se autentique antes de prosseguir com a configuração dos protocolos de rede (fase NCP). Neste estado são negociadas opções através de pacotes LCP com base num protocolo de autenticação específico, daí que a autenticação não seja obrigatória.

Este estado só pode ser activado quando é recebido um sinal explícito de indicação do término do estado de estabelecimento. Se a autenticação for obtida com sucesso a linha passa para o estado de Rede, no caso de insucesso a ligação retorna para o estado de terminação.

Os protocolos permitidos neste estado são o LCP, os protocolos de monitorização de linha e os protocolos de autenticação.

2.3.4 Estado de Rede

Uma vez terminado o estado precedente, cada protocolo de rede (tais como o IP, IPX e AppleTalk) deve ser configurado separadamente pelo protocolo NCP correspondente, que no caso do IP é o IPCP.

Quando o estado de Rede termina o protocolo de rede negociado é o assumido no estado de Aberto. Qualquer outro protocolo de rede diferente do configurado ao ser recebido deverá ser imediatamente descartado. Neste estado qualquer combinação de pacotes como LCP, NCP ou outros protocolos de rede podem surgir.

2.3.5 Estado de Aberto

Neste estado a transferência de dados é possível, correspondendo ao nível IP do protocolo TCP/IP. Terminado este estado a máquina de estados transita para o estado de Terminação.

2.3.6 Estado de Terminação

O PPP pode terminar a ligação em qualquer altura. Isto pode acontecer devido a perda da portadora, falha na autenticação, fraca qualidade de ligação, um temporizador expirado por causa de um período longo de inactividade e ainda o encerramento por parte do operador.

O LCP faz a troca de pacotes de terminação da ligação. Quando a troca de pacotes de terminação da conexão chega ao fim é necessário forçar a camada física à desconexão, particularmente quando há falha de autenticação.

O remetente do pacote *Terminate-Request* deve desligar após receber um pacote *Terminate-Ack* ou depois do temporizador expirar. Finalmente o PPP prossegue para o estado inactivo. Caso os pacotes do tipo LCP sejam recebidos devem ser imediatamente descartados.

2.4 Protocolo LCP

O protocolo de controlo de ligação LCP permite iniciar a ligação, testar a qualidade da linha, negociar opções de configuração, como por exemplo o tipo de protocolo a ser usado nas fases seguintes, e finalmente interromper a ligação quando esta já não seja necessária.

Existem três classes de pacotes LCP a saber:

1. Pacotes de configuração da ligação, que são usados para estabelecer e configurar a ligação *(Configure-Request, Configure-Ack, Configure-Nak e Configure-Reject).*
2. Pacotes terminadores de ligação, que são usados para terminar a ligação *(Terminate-Request, Terminate-Ack).*
3. Pacotes para manutenção, controle e eliminação de erros da ligação *(Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply e Discard-Request).*

2.4.1 Formato de pacotes LCP

O pacote LCP é encapsulado em tramas PPP como é mostrado na Figura 8.

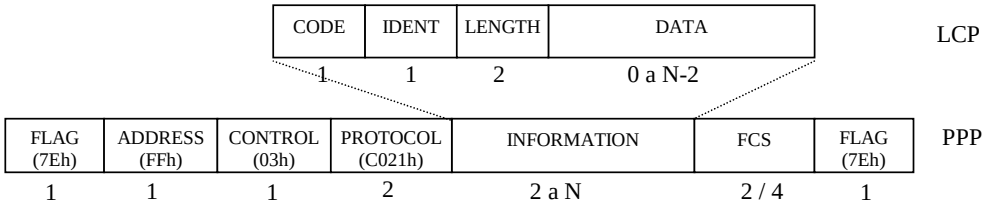

Figura 8 - Pacote LCP

O protocolo LCP é identificado pelo valor $C021_h$ no campo **Protocol**, sendo constituído pelos campos **Code, Identifier, Length** e **Data.**

O campo **Code** ocupa um octeto e contém valores que variam de um a onze, de identificação do pacote LCP. Caso o pacote seja recebido com campo **Code** desconhecido é rejeitado e enviado um pacote *code-reject.* De acordo com o IANA existem onze tipos de pacotes LCP e duas extensões (definidas na RFC 1570), que podemos observar na Tabela 4.

Tabela 4 – *Descrição dos pacotes LCP*

Code	Nome	Sentido	Descrição
1	Configure-Request	T-->R	Pacote com proposta de opções de configuração da linha com respectivos valores.
2	Configure-Ack	T←R	Resposta com indicação de aceitação de todas as opções.
3	Configure-Nak	T←R	Se as opções tiverem valores diferentes das suportados pelo R, este responde apenas com especificação de valores suportados.
4	Configure-Reject	T←R	Se as opções propostas não forem suportadas por R, este responde enviando um pacote com todas as opções e valores que não suporta.

5	Terminate-Request	T→R	Pedido de término da ligação, é enviado insistentemente até que chegue um pacote *Terminate-Ack* como resposta.
6	Terminate-Ack	T←R	R envia este pacote sobre a recepção de um pacote *Terminate-Request*, como confirmação do fim da ligação.
7	Code-Reject	T←R	Se o pacote LCP tiver o campo **Code** desconhecido, R responde com a cópia desse pacote LCP.
8	Protocol-Reject	T←R	Se o pacote LCP tiver o campo **Protocol** desconhecido significa que T tenta usar um protocolo que R não suporta, então é enviado um pacote com a cópia desse pacote.
9	Echo-Request	T→R	Este pedido é enviado para que T saiba que não está a comunicar com ele próprio, envia a opção **magic-number** no pacote *echo-request.*
10	Echo-Reply	T←R	Resposta positiva ao pacote *echo-request*
11	Discard-Request	T←→R	Pacote enviado para o terminal remoto para testes de ligação entre outras funções.
12	Identification	T←→R	Pacote enviado para identificação junto do interlocutor.
13	Time-Remaining	T←→R	Pacote enviado para indicar o tempo remanescente na ligação.

O terminal T inicia a ligação propondo certas opções de configuração do tipo LCP ao terminal R, e consoante o tipo de opção este envia respostas adequadas à proposta recebida. Existem também pacotes para terminar a ligação que podem ser enviados por qualquer um dos terminais.

O campo **Identifier** relaciona a sequência das mensagens transmitidas com as mensagens recebidas. O campo **Length** tem dois octetos, indicando o tamanho total do pacote LCP incluindo o cabeçalho. O campo **Data** tem tamanho variável, dependente do código do pacote.

2.4.2 Opções de configuração de pacotes LCP

Como foi referido os pacotes LCP contêm uma série de opções a serem negociadas. Pretende-se que as opções de configuração do protocolo PPP sejam fáceis de negociar, devendo as opções configuradas ser mantidas após a negociação. Consideram-se também as opções de configuração com a intervenção do operador que de outra forma seriam impossíveis de realizar, como por exemplo os dados para a autenticação do utilizador ou a atribuição dinâmica de endereços IP. A configuração automática é conseguida graças a um mecanismo extensivo de negociação de opções, baseada numa máquina de estados.

Exemplifica-se em seguida a sequência de mensagens entre dois terminais, considerando um terminal cliente a que chamamos Cliente e um servidor de Internet designado por ISP.

Quando se dá o início das negociações para a configuração da ligação, o Cliente envia um pacote *configure-request* com uma lista de opções que suporta, propondo ao ISP que as suporte também, e quase simultaneamente o ISP envia um pacote *configure-request* com a respectiva lista de opções definidas por omissão. Este comportamento justifica-se pelo facto das máquinas de estado de ambos serem iguais e se iniciarem a partir do instante em que o meio físico se torna disponível.

As negociações prosseguem até que ambos recebam pacotes *configure-ack* , confirmando a chegada a um acordo. Este acordo pode demorar se pelo meio houver opções que não são aceites por qualquer um dos terminais, o que é mais frequente. Em resposta são enviados pacotes *configure-reject* ou *configure-nak* de acordo com a descrição da Tabela 4.

A Figura 9 mostra a estrutura de dados do pacote de configuração de opções de LCP.

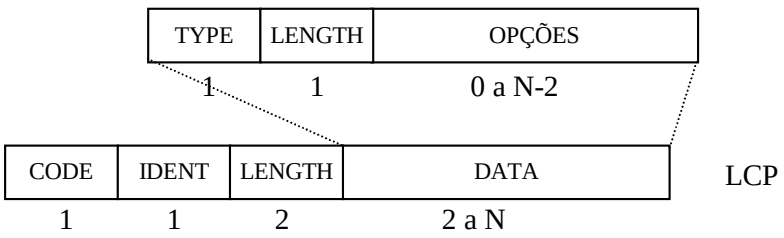

Figura 9 - Estrutura do pacote de opções de configuração de LCP

O campo **Type** ocupa um octeto e admite valores especificados no IANA, o campo **Length** ocupa um octeto e contêm o tamanho em bytes da opção incluindo **Type, Length** e **Data**, o campo **Data** ocupa um espaço variável dependendo do valor da opção como mostra a Tabela 5.

Tabela 5 - Opções de Configuração de LCP

Type	Descrição
0	Vendor Specific [RFC2153]
1	Maximum Receive Unit
2	Async-Control-Character-Map
3	Authentication-Protocol
4	Quality Protocol
5	Magic-Number
7	Protocol Field Compression
8	Address and Control Field Compression
9	FCS-Alternatives [RFC1570]

Apresenta-se em seguida uma descrição sucinta de algumas opções de configuração.

Maximum Receive Unit (MRU)

É uma opção que é enviada ao *peer* para configurar o tamanho dos pacotes PPP. Por opção este número é colocado em 1500 bytes. Se for negociado o envio de números inferiores a implementação deve poder suportar os 1500 bytes no caso da sincronização da ligação ser perdida.

Authentication Protocol

É uma opção que é exigida por quase todos os provedores de Internet que requerem uma autenticação antes de começarem a receber e enviar pacotes do nível três do modelo de referência OSI. Devido a existirem diferentes tipos de protocolos para autenticação, é negociado um protocolo específico de autenticação. Por opção a autenticação não é requerida.

Um pacote *Configure-Request* não deve incluir opções múltiplas de protocolos de autenticação, no caso de não ser aceite o valor da opção através de um pacote *Configure-Nak*, uma nova tentativa pode ser feita enviando um novo valor de preferência e assim sucessivamente.

Quality-protocol-report

É uma opção que permite monitorar durante a ligação eventuais perdas de dados. Os meios físicos estão sujeitos a influências externas que levam ao ponto das ligações nunca serem fiáveis, pelo que é conveniente ter estatísticas de perdas de dados.

Magic Number

É uma opção que implementa um mecanismo de detecção de retorno de sinais emitidos permitindo que o *peer* saiba que não está a comunicar consigo próprio mas com a rede, entre outras anomalias da ligação de dados. Por opção o *Magic-Number* não é negociado, mas se este for pedido pelo *peer* deve-se responder com a escolha de um número o mais aleatório possível, de modo a garantir uma elevada probabilidade de ser diferente do *peer*. Recomenda-se que o número mágico seja o mais original possível tal como a data do dia, o número de série da máquina, *etc.*

Se um pacote *Configure-Request* com a opção *Magic-Number* for rejeitada com um pacote *Configure-Reject* assume-se que não existem retornos e que os pacotes que usam este número como *Echo-Request* devem ser silenciosamente descartados.

Protocol Field Compression (PFC)

É uma opção que implementa um método especifico de compressão do campo protocolo PPP. Opcionalmente todos os pacotes devem transmitir o campo **protocol** com dois Octetos.

Neste protocolo os números devem ser escolhidos de forma a assentar sobre um formato de um octeto, e que seja claramente distinto do formato de dois octetos. Esta opção serve para informar ao *peer* que pode receber pacotes com o campo **protocol** com apenas um octeto.

Este protocolo é baseado no método de extensão de endereços normalizado na recomendação [ISO-3309].

Address and Control Field Compression (ACFC)

Esta opção oferece um método de compressão dos campos **Address** e **Control** no nível de ligação de dados. Por omissão todas as tramas devem ser transmitidas com os campos *Address* e *Control* em octetos individuais.

Se esta opção for negociada todos as tramas devem ser trocadas com os dois campos comprimidos, porque caso contrário podem surgir erros de FCS e a comunicação torna-se inviável.

FCS Alternatives

Esta opção oferece a possibilidade de configurar várias alternativas de formato de FCS. Esta opção é negociada separadamente em cada direcção. Estão definidas 3 opções de FCS:

1 FCS nulo;

2 FCS ITU-T 16 bit

4 FCS ITU-T 32 bit

Na maioria das implementações o FCS por omissão é ITU-T 16 bit. O FCS nulo deve ser usado só no caso de a camada de rede ou de transporte terem mecanismos de checksum extremo a extremo, tal como e´o caso de TCP/IP ou UDP/IP com o checksum activado.

2.5 Protocolos de autenticação

Existem dois tipos de protocolos de autenticação mais usados, o PAP (*Password-Authentication-Protocol*) [RFC1334] e o CHAP (*Challenge-Handshake-Authentication-Protocol*) [RFC1333]. O mais comum entre os provedores de Internet é o PAP devido à sua maior simplicidade.

2.5.1 PAP (Password Authentication Protocol)

O PAP é um método simples de autenticação em que a identificação é feita num sentido e no sentido de retorno aguarda-se uma única resposta de aceitação ou rejeição, e é feita apenas no início do estabelecimento de uma ligação PPP.

O processo de autenticação PAP tem início depois de terminado o estado de estabelecimento descrita anteriormente, onde o utilizador envia uma combinação nome_do_utilizador / palavra_chave para a entidade autenticadora, e espera que uma resposta seja devolvida, caso contrário a ligação termina.

Este é um protocolo em que os dados são enviados em texto puro e o utilizador tem um controlo total relativamente à frequência e ao número de tentativas de autenticação.

O protocolo PAP é encapsulado na trama PPP do mesmo modo que é o protocolo LCP mas com a diferença de não ter campos extensivos de opções de configuração no campo **Data.** No campo **Protocol** é usado o valor $C023_{hex}$ que identifica o protocolo PAP.

A Figura 10 mostra a estrutura de dados do pacote *authenticate-request.* Trata-se do pacote mais importante do protocolo PAP, por conter os elementos de identificação do utilizador.

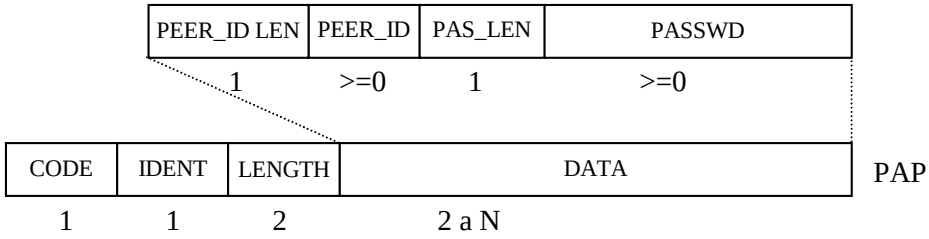

Figura 10 - Pacote PAP Authenticate Request

O campo **Code** ocupa um octeto e identifica o tipo de pacote PAP. No caso deste campo não ser reconhecido o pacote é imediatamente descartado.

De acordo com o RFC1334 existem três tipos de pacotes PAP, como é mostrado na Tabela 6, que toma como exemplo a comunicação em que existe uma troca de pacotes sucessiva entre T e R.

Tabela 6 - ***Pacotes PAP e sua descrição***

Code	Nome	Sentido	Descrição
1	Authenticate-request	T->R	Pacote utilizado para iniciar o protocolo PAP, que ser enviado repetidamente dentro de um número definido de tentativas ou então activando um relógio até que seja recebida a resposta.
2	Authenticate-ack	T<-R	Confirmação da validade da combinação *username/password* recebido do pacote *Authenticate-Request*
3	Authenticate-nak	T<-R	Rejeição da combinação username/password recebido do *Authenticate-Request*

A autenticação inicia-se quando T envia um pacote *authenticate-request* com elementos de autenticação constituído pela combinação do nome do utilizador e palavra chave. Depois de R receber estes dados compara-os com os que estão armazenados na sua base de dados e responde com pacote *authenticate-ack* se forem validos,ou *authenticate-nak* no caso contrário.

O campo **Code** ocupa um octeto, e é preenchido com o valor do protocolo de autenticação negociado no estado configuração da ligação de dados (LCP).

O campo **Identifier** ocupa um octeto, e é preenchido por números que relacionam a sequência das mensagens transmitidas com as mensagens ou pacotes recebidos.

O campo **Length** ocupa dois octetos, indica o tamanho em bytes do pacote PAP, que inclui os campos **Code ,Identifier, Length e Data.**

No caso de um pacote *authenticate-request*, como mostra a Figura 10, o campo **Data** é ocupado pelos seguintes elementos.

- **Peer_ID_length** : ocupa um octeto é indica o tamanho em bytes do campo **Peer_ID**.
- **Peer_ID** : tem zero ou mais octetos e é preenchido pelo nome do utilizador a ser autenticado.
- **Passwd_length** : ocupa um octeto e indica o tamanho em bytes do campo Passwd.
- **Passwd** : ocupa zero ou mais octetos e é preenchido pela palavra chave do utilizador a ser autenticada. O pacote *authenticate-ack* e *authenticate-nak* têm o campo **Data** vazio, a entidade autenticadora encarrega-se apenas de dar a indicação de ter aceite ou rejeitado respectivamente o pacote *authenticate-request.*

2.5.2 CHAP (Challenge Handshake Authentication Protocol)

O CHAP [RFC1994] é um protocolo de autenticação usado para a verificação periódica da identidade do *peer* remoto pelo método "3-way handshake" no início do estabelecimento da ligação e depois em qualquer altura depois do link estar estabelecido.

De acordo com o RFC1994 existem 4 tipos de pacotes CHAP, como é mostrado na Tabela 7.

Tabela 7 - ***Pacotes CHAP e sua descrição***

Code	Nome	Sentido	Descrição
1	Challenge	T<-R	Pacote enviado pelo autenticador para iniciar o protocolo CHAP. Pode ser enviado repetidamente um número definido de tentativas ou até expirar um temporizador, até que seja recebida a resposta.
2	Response	T->R	Pacote enviado como resposta ao pacote Challenge. Sempre que um pacote da resposta é recebido, o autenticador compara o valor da resposta com seu próprio cálculo do valor previsto.
3	Success	T<-R	Pacote enviado pelo autenticador se o valor da resposta for correcta.
4	Failure	T<-R	Pacote enviado pelo autenticador se o valor da resposta for incorrecta.

O método "3-way handshake" consiste no envio de uma mensagem *challenge* pelo equipamento autenticador ao equipamento remoto, e este responde com uma mensagem calculada na base de uma função "one-way hash". A resposta é analisada e, se os valores coincidirem, uma resposta de confirmação é enviada, caso contrário a ligação termina. Os valores são únicos e secretos, e são apenas do conhecimento da entidade autenticadora e do equipamento remoto.

O valor do desafio é uma sequência variável de octetos. O valor do desafio deve ser mudado cada vez que um desafio é emitido. O comprimento do valor do desafio depende do método usado gerar os octetos, e é independente do algoritmo de *hash* usado.

O valor da resposta é o *hash* calculado sobre uma sequência de octetos que consistem no identificador, concatenado com o "segredo", concatenado com o valor do desafio. O comprimento do valor da resposta depende do algoritmo *hash* usado (16 octetos para MD5).

Na figura Figura 11 apresenta-se um diagrama de mensagens exemplificativo do funcionamento do protocolo CHAP.

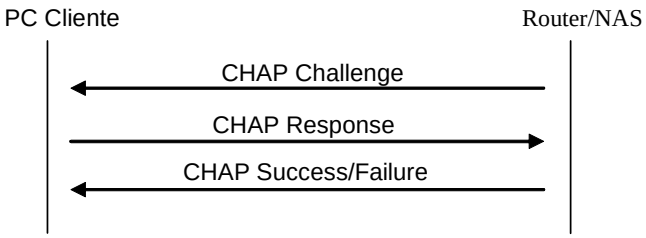

Figura 11 – Diagrama de mensagens do protocolo CHAP

2.6 Protocolo IPCP

Na presente implementação o NCP configura protocolos do tipo IP especialmente para permitir o acesso a Internet. A negociação do protocolo IP é denominada Internet Protocol Control Protocol (IPCP) [RFC1332].

O IPCP é responsável em ambos os extremos da ligação pela capacidade de utilização ou não do uso de pacotes do tipo IP. O IPCP usa o mesmo mecanismo de troca de pacotes de controle de ligação (LCP) descrito anteriormente. Pacotes IPCP não podem ser trocados até que o estado de configuração de protocolos de rede (NCP/IPCP) seja alcançada. Os pacotes IPCP recebidos antes deste nível ser atingido devem ser silenciosamente descartados.

Os pacotes IPCP têm a mesma constituição que os pacotes LCP na sua estrutura de dados e funcionamento, com algumas excepções a considerar:

- Ao nível de ligação de dados o pacote IPCP é encapsulado no campo **Information** da trama PPP, onde o campo **Protocol** é preenchido pelo 8021_{hex} [IANA].

- O campo **Code** admite sete pacotes IPCP: *configure-request*, *configure-ack*, *configure-nak*, *configure-reject*, *terminate-request*, *terminate-ack* e *code-reject*. Qualquer outro código deve ser rejeitado.

- Só poderão ser trocados pacotes IPCP após terminadas as fases de estabelecimento de linha e de autenticação.

2.6.1 Descrição das opções de configuração IPCP

O IPCP apresenta uma série de opções de configuração como mostra a Tabela 7.

Tabela 8 - ***Opções de configuração IPCP***

Tipo	Descrição	Comprimento (bytes)	Valor (Hex)
2	IP Compression Protocol [RFC1144]	>=4	002d
3	IP Address	6	Variável
129	Primary DNS [RFC1877]	6	Variável
130	Secundary DNS [RFC1877]	6	Variável
131	Primary NBNS [RFC1877]	6	Variável
132	Secundary NBNS [RFC1877]	6	Variável

IP Compression Protocol

É uma opção que ocupa dois octetos e indica o tipo de compressão do protocolo desejado. Por opção a compressão não está activada.

A compressão de cabeçalho TCP/IP Van Jacobson (RFC 1144) permite reduzir o tamanho dos cabeçalhos TCP/IP de 40 octetos para 3 octetos, o que é um aumento significativo da eficiência e redução do tempo de transmissão dos pacotes, em especial para pacotes com campo de informação baixo e canais de baixo débito.

É possível definir várias opções na transmissão de pacotes IP, identificadas através do campo Protocol do PPP que se indicam na Tabela 9.

Tabela 9 – Valores do campo Protocolo de PPP para transmissão de pacotes IP

Valores (hex)	Protocolos
0021	IP - Pacote IP com cabeçalho não comprimido
002d	TCP/IP com cabeçalho comprimido
002f	TCP não comprimido, IP comprimido

IP Address

É uma opção que ocupa quatro octetos e possui uma forma de negociação de endereços IP a ser usado pelo utilizador remoto ao longo da ligação. Permite que o remetente especifique que endereço IP deseja utilizar. O *peer* pode responder com um pacote *Configure-Nak* com o valor IP válido a ser usado. O requerente remoto pode sugerir um endereço IP ou pode enviar um endereço a zero, para que o *peer* atribua um endereço IP.

Primary DNS (Domain Name Server)

Esta opção é do tipo 129. Define o método de negociação do endereço Primary DNS com o *peer* remoto a ser usado no terminal.

Se o *peer* local enviar um endereço ao servidor com valor falso (que normalmente é feito intencionalmente), o servidor retorna um pacote Nak que contém o valor Primary DNS correcto.

Secundary DNS (Domain Name Server)

Esta opção define o método de negociação do endereço Secondary DNS com o *peer* remoto a ser usado no terminal.

Se o *peer* local enviar um endereço ao servidor com valor falso (que normalmente é feito intencionalmente), o servidor retorna um pacote Nak que contém o valor Secondary DNS correcto.

Primary NBNS (Netbios Name Server)

Esta opção define o método de negociação do endereço Primary NBNS com o *peer* remoto a ser usado no terminal.

Se o *peer* local enviar um endereço ao servidor com valor falso (que normalmente é feito intencionalmente), o servidor retorna um pacote Nak que contém o valor Primary NBNS correcto.

Secundary NBNS (Netbios Name Server)

Esta opção define o método de negociação do endereço Secondary NBNS com o *peer* remoto a ser usado no terminal.

Se o *peer* local enviar um endereço ao servidor com valor falso (que normalmente é feito intencionalmente), o servidor retorna um pacote Nak que contém o valor Secondary NBNS correcto.

2.6.2 Envio de Pacotes IP

Antes de qualquer pacote IP ser transmitido, o IPCP deve alcançar o estado *Opened* na fase de configuração de protocolos de rede (NCP).

Um pacote do tipo IP é encapsulado exactamente numa trama PPP, com a indicação 0021_{hex} no campo Protocolo.

O comprimento máximo de um pacote IP deve ser o mesmo que o tamanho máximo do campo **Information** da trama PPP. Os datagramas maiores devem ser fragmentados quando necessário.

Se o sistema desejar evitar a fragmentação e a reagrupamento de pacotes, deverá usar a opção do tamanho máximo do TCP e da MTU.

2.7 Diagrama de opções LCP

O diagrama seguinte mostra a maioria dos parâmetros LCP que podem ser negociados durante a fase de estabelecimento. Este diagrama pode ajudar a localizar os parâmetros LCP que a máquina local não está a negociar com a máquina LCP remota.

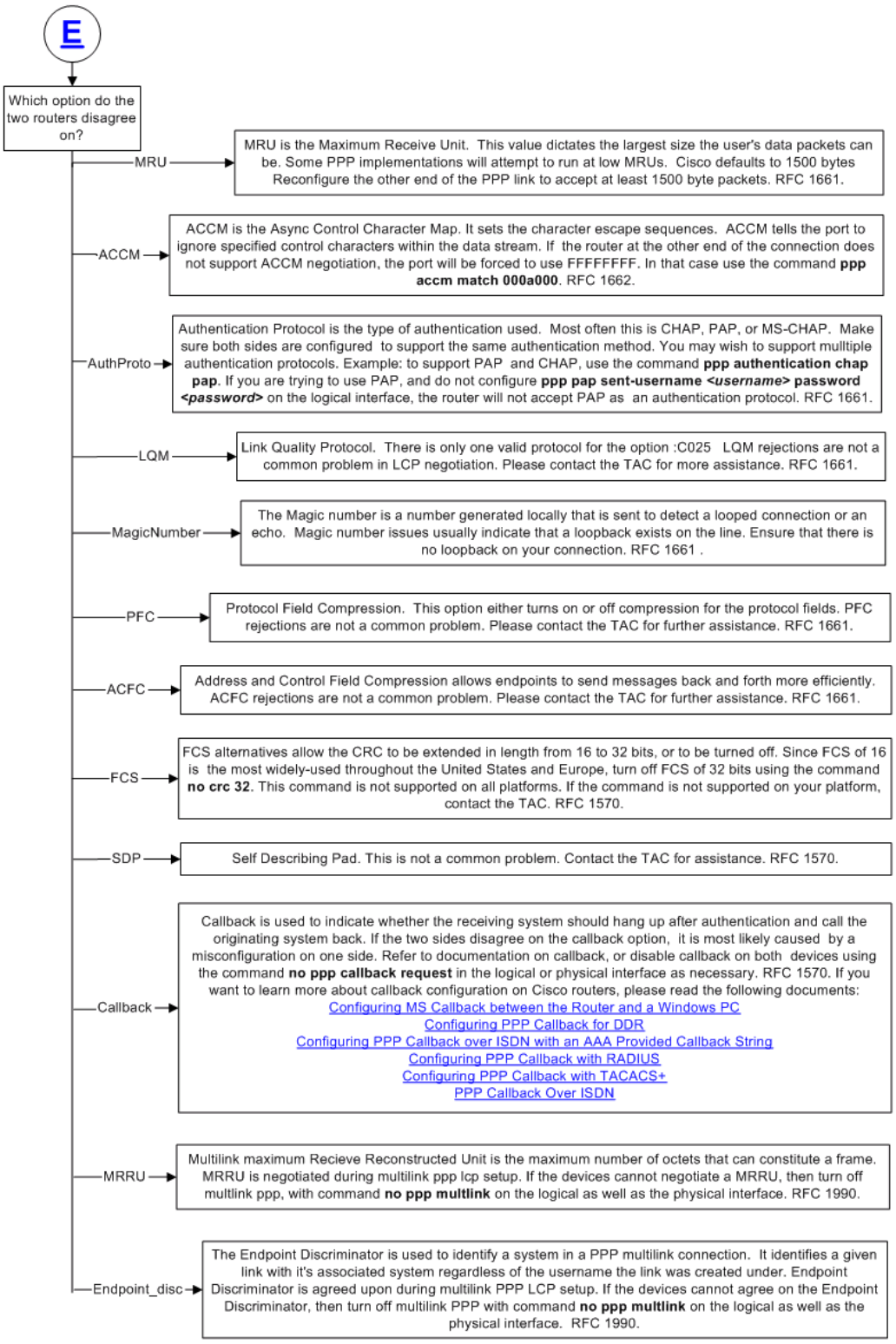

Figura 12 – Diagrama de opções de estabelecimento PPP [CISCO]

2.8 O protocolo PPP Multilink

As interfaces básica e primária de RDIS oferecem a possibilidade de abrir múltiplos canais simultâneos entre equipamentos terminais, dando aos utilizadores largura de banda a pedido, obviamente com custos adicionais.

Há várias propostas que proporcionam sincronização entre múltiplos fluxos ao nível de bit, de que se destaca a proposta BONDING, mas que têm o inconveniente de requererem hardware adicional.

A solução definida na RFC 1990, "The PPP Multilink Protocol (MP)", pode ser implementada inteiramente em software, sendo baseada num cabeçalho de 4 octetos e em regras simples de re-sincronização.

Na Figura 13 apresenta-se um diagrama esquemático do funcionamento do PPP Multilink.

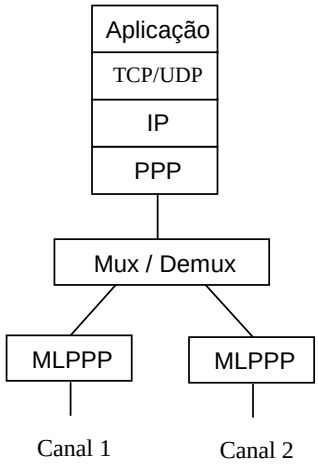

Figura 13 – Diagrama de funcionamento do PPP Multilink

São definidos dois formatos de tramas que diferem no tamanho do número de sequência. Na Figura 14 apresenta-se a estrutura dos pacotes MP com Número de Sequência Longo.

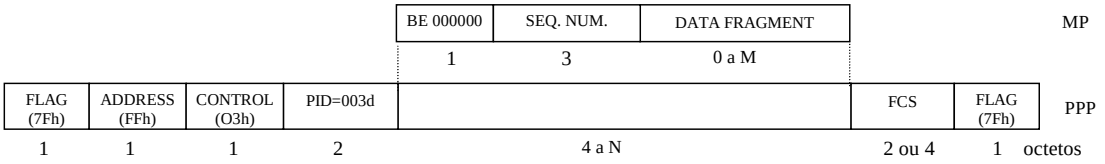

Figura 14 – Formato PPP Multilink com Número de Sequência Longo

Na Figura 15 apresenta-se a estrutura dos pacotes MP com Número de Sequência Curto.

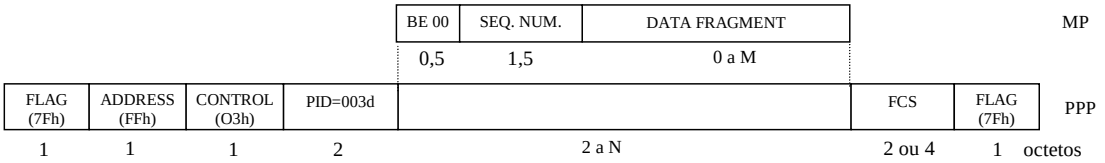

Figura 15 – Formato PPP Multilink com Número de Sequência Curto

O bit B (*Beginning*) é posto a 1 no primeiro fragmento derivado do pacote PPP e posto a 0 para todos os outros fragmentos do pacote PPP.

O bit E (*Ending*) é posto a 1 no último fragmento derivado do pacote PPP e posto a 0 para todos os outros fragmentos do pacote PPP.

Na Figura 16 exemplifica-se a segmentação de um pacote PPP em dois fragmentos MP, em que se constata que o primeiro fragmento de MP contém dois cabeçalhos, o primeiro de MP e o segundo de PPP. Como se vê na figura, o identificador do protocolo PPP-ML é 003d.

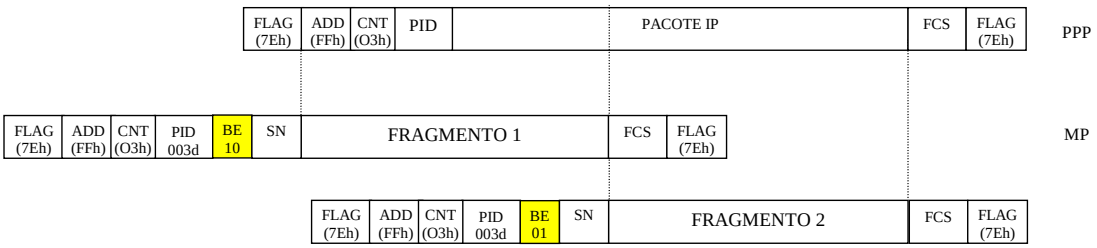

Figura 16 – Exemplo de segmentação de pacote PPP em dois fragmentos MP

2.9 Extensão Multi-Classe para PPP Multilink

Na RFC 2686 foi definida uma extensão de PPP Multilink para suportar serviços integrados sobre linhas de baixo débito. Para tal é definido um formato de encapsulamento para tempo real, baseado no mecanismo de fragmentação do PPP Multilink, a que se adiciona o campo CLS (Classe) que permite definir pacotes com diferentes prioridades e diferentes disciplinas de serviço.

Na Figura 17 apresenta-se a estrutura dos pacotes MP com Classes com Número de Sequência Longo, em que o campo CLS tem a dimensão de 4 bits.

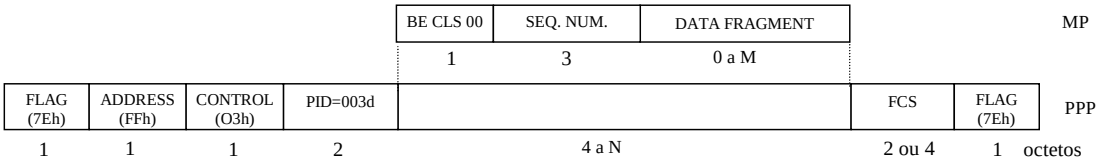

Figura 17 – Formato PPP Multilink com Classes com Número de Sequência Longo

Na Figura 18 apresenta-se a estrutura dos pacotes MP com Classes com Número de Sequência Curto, em que o campo CLS tem a dimensão de 2 bits.

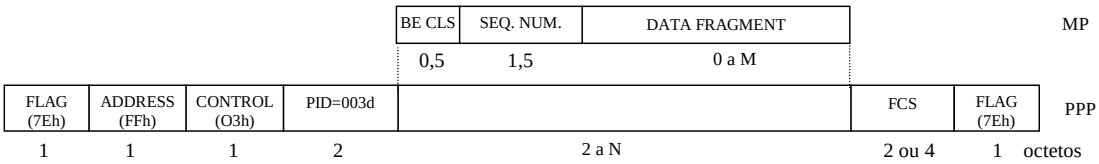

Figura 18 – Formato PPP Multilink com Classes com Número de Sequência Curto

2.10 PPP sobre RDIS

Na RFC 1618 “PPP over ISDN” é descrita a utilização do encapsulamento PPP sobre ligações RDIS.

O PPP trata os canais RDIS como ligações síncronas orientadas ao bit ou ao octeto.

Na ausência de configuração específica, a implementação deve usar em primeiro lugar HDLC síncrono ao bit. Como alternativa pode ser usado HDLC síncrono ao octeto

Para o canal D pode ser usado o encapsulamento em X.25 ou em Frame Relay, definidos respectivamente na RFC 1598 “PPP in X.25 ou a RFC 1973 “PPP in Frame Relay”.

2.10.1 Encapsulamento de PPP em X.25

O encapsulamento de PPP em X.25 definido na RFC 1598 é mostrado na Figura 19.

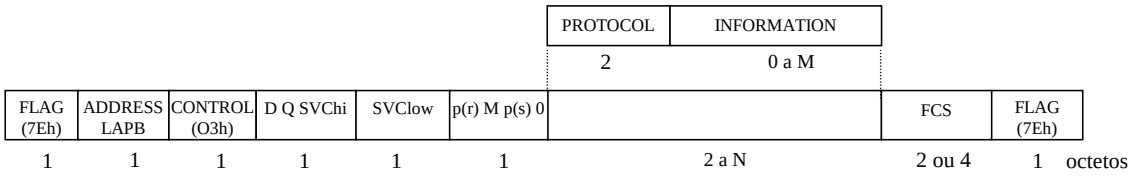

Figura 19 – Formato PPP em X.25

No caso do canal D de RDIS o formato de PPP é análogo ao da figura, apenas difere o campo de endereço, em que o endereço LAPB é substituído pelo endereço LAPD.

2.10.2 Encapsulamento de PPP em Frame Relay

O encapsulamento de PPP em Frame Relay definido na RFC 1973 é mostrado na Figura 20.

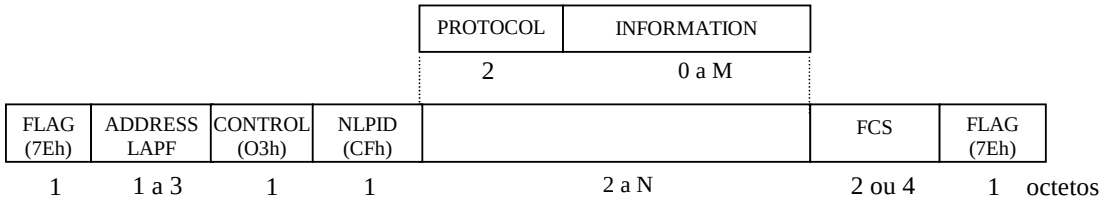

Figura 20 – Formato PPP em Frame Relay

Verificam-se duas alterações em relação ao formato comum do PPP, o campo de endereço LAPF e o campo NLPID (*Network Layer Protocol Identifier*), que identifica o encapsulamento que se segue.

No caso do canal D de RDIS o formato de PPP é análogo ao da figura, apenas difere o campo de endereço, em que o endereço LAPF é substituído pelo endereço LAPD.

2.11 PPP sobre ATM

O acesso às redes IP através de ATM, como é o caso da tecnologia de acesso ADSL, leva à necessidade de definir a utilização de PPP sobre ATM, utilizando eventualmente diferentes camadas AAL. O PPP sobre AAL5 já se encontra definido no RFC 2364, enquanto que o AAL2 está definido no RFC 3336.

2.11.1 PPP sobre AAL5

O RFC 2364, "PPP over AAL5", define a utilização de PPP sobre ATM usando o AAL5, nomeadamente os mecanismos de encapsulamento de PPP em PDUs AAL5.

Para transporte de PPP sobre AAL5 é adoptada a estrutura de trama definida na RFC 1483, sendo escolhido o método de Encapsulamento por LLC.

O formato de encapsulamento de pacotes PPP em AAL5 é apresentado na Figura 22.

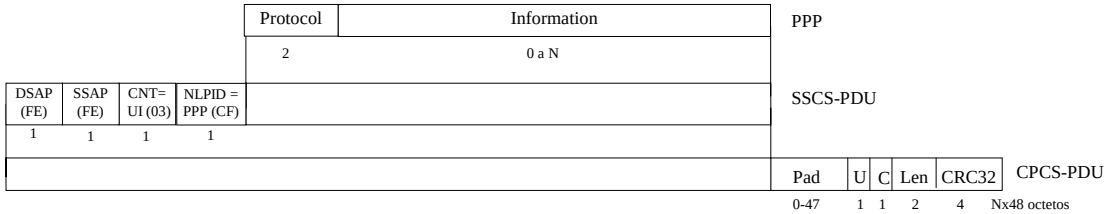

Figura 21 - Encapsulamento PPP em AAL5

Como se pode constatar, as Flags e o CRC de HDLC são eliminados, uma vez que não são necessários no encapsulamento em AAL5.

É adicionado ao pacote PPP um cabeçalho LLC, constituído pelos campos DSAP (Destination Service Access Point), SSAP (Source Service Access Point) e Control (trama UI), aos quais se adiciona o campo NLPID (*Network Layer Protocol Identifier*), que identifica o encapsulamento que se segue como PPP.

Na cauda utiliza-se a cauda usual da subcamada CPCS de AAL5, constituída pelo Pad de tamanho variável e pelos campos UU (*User-User Information*), CPI (*Common Part Indicator*), Len (*Length*) e CRC32.

2.11.2 PPP sobre AAL2

O RFC 3336 "PPP over AAL2", define a utilização de PPP sobre ATM usando o AAL2, nomeadamente os mecanismos de encapsulamento de PPP em PDUs AAL2.

O encapsulamento do PPP usando SSSAR (*Service Specific Segmentation and Reassembly*) e AAL2 CPS (*Common Part Sublayer*) é mais eficiente que o AAL5. Utilizando um CRC de 2 octetos e considerando que o cabeçalho do CPS de AAL2 é de 3 octetos e o campo Offset é de 1 octeto, obtemos um "overhead" de encapsulamento de 6 octetos, o que é inferior aos 8 octetos da cauda do AAL5.

A função de multiplexagem de subcamada CPS de AAL2 permite ainda uma maior eficiência de transporte de pacotes, multiplexando múltiplos pacotes em uma ou mais células, eliminando o "overhead" do Pad de AAL5, o que particularmente importante no transporte de pacotes pequenos.

O formato de encapsulamento de pacotes PPP em AAL2 é apresentado na Figura 22.

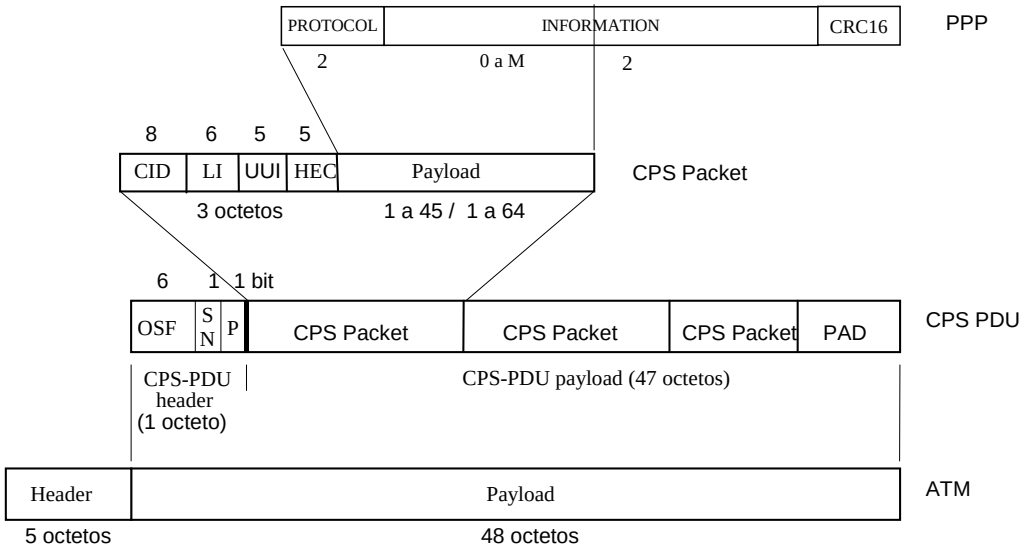

Figura 22 - Encapsulamento PPP em AAL2

Como se pode observar na figura, o pacote PPP possui um CRC de 16 bits. O campo CID (*Channel Identifier*) do pacote CPS é de 8 bits, o LI (*Length Indicator*) é de 6 bit, UUI (*User-to-User Indication*) é de 5 bit e HEC (*Header Error Control*) é de 5 bit, num total de 3 octetos.

No caso do pacote PPP exceder 45 octetos (ou 64), há fragmentação em vários pacotes CPS, sendo usado o campo UUI para indicar o fim do pacote PPP: se não for fim de pacote PPP o UUI=27, se for fim de pacote o UUI=26.

2.12 PPP sobre Ethernet

O PPP sobre Ethernet (PPPoE), definido na RFC 2516, pretende fornecer as facilidades definidas para PPP em ligações ponto-a-ponto para o ambiente multi-ponto disponível na Ethernet e em outros ambientes de acesso múltiplo.

O PPPoE permite conectar um conjunto de terminais sobre um simples acesso de *bridging* a um concentrador de acesso remoto. Com este modelo, cada terminal utiliza a sua pilha PPP e é apresentada ao utilizador uma interface familiar. O controlo de acesso, a facturação e o tipo de serviço podem ser feitos numa base de utilizador, em vez ter por base o local.

Para fornecer uma conexão ponto a ponto sobre a Ethernet, cada sessão PPP deve aprender o endereço Ethernet do par remoto, assim como estabelecer um identificador de sessão único. O PPPoE inclui um protocolo de descoberta que providencia esta funcionalidade.

O PPPoE tem duas fases distintas, a fase de Descoberta e a fase de Sessão PPP. Quando um terminal pretende iniciar uma sessão PPPoE, deve em primeiro lugar executar a Descoberta para identificar o

endereço MAC da Ethernet do par e estabelecer um identificador de sessão PPPoE. Enquanto que o PPP define uma relação entre pares, a Descoberta define uma relação cliente-servidor. No processo de Descoberta, um terminal (cliente) pode descobrir um ou mais concentrador do acesso (servidores), seleccionando um de entre eles. Quando a Descoberta termina com sucesso, o terminal e o concentrador de acesso seleccionado têm a informação que usarão para construir a sua conexão ponto a ponto sobre a Ethernet.

A fase de Descoberta permanece sem estado até que uma sessão do PPP esteja estabelecida. Uma vez estabelecida uma sessão PPP, o terminal e o concentrador do acesso devem atribuir os recursos para uma interface virtual PPP.

Na Figura 23 mostra-se o formato de uma trama PPPoE, a qual ocupa o campo de informação de uma trama Ethernet.

VER	TYPE	CODE	SESSION_ID	LENGTH	PAYLOAD
1/2	1/2	1	2	2	N octetos

Figura 23 – Formato das tramas PPPoE

O campo VER que indica a versão do PPPoE deve ser colocado a 0x1 O campo TYPE deve ser também colocado a 0x1. O campo CODE é definido para as fases de Descoberta e de sessão do PPP

O campo SESSION_ID é um valor definido para pacotes de Descoberta. O seu valor é fixado para uma determinada sessão de PPP e define uma sessão PPP juntamente com os endereços MAC de origem e destino da Ethernet.

O campo LENGTH indica o comprimento do payload de PPPoE. Não inclui o comprimento dos cabeçalhos de Ethernet ou de PPPoE.

Há quatro etapas na fase da Descoberta, no fim da qual ambos os pares conhecem a SESSION_ID PPPoE e o endereço Ethernet do par, que em conjunto definem univocamente a sessão PPPoE. As quatro etapas da Descoberta consistem no seguinte, tal como se ilustra na Figura 24:

1. O terminal transmite em broadcast um pacote de iniciação (PPPoE Active Discovery Initiation, PADI);
2. Um ou mais concentradores de acesso (AC) emitem pacotes de oferta (PPPoE Active Discovery Offer, PADO);
3. O terminal emite um pacote do pedido da sessão em unicast ao concentrador de acesso seleccionado (PPPoE Active Discovery Request, PADR);
4. O concentrador de acesso seleccionado emite um pacote da confirmação (PPPoE Active Discovery Session-confirmation, PADS).

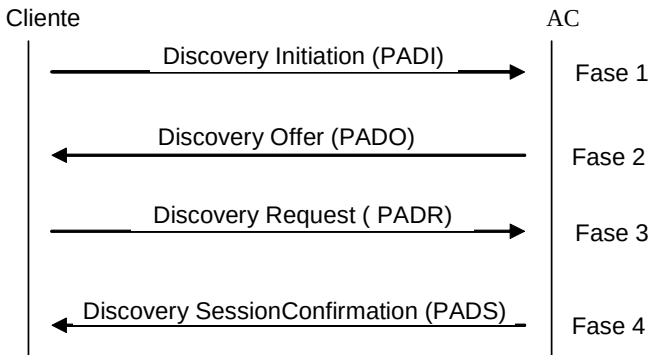

Figura 24 – Fases de Descoberta PPPoE

Quando o terminal recebe o pacote da confirmação, pode prosseguir para a fase de sessão do PPP. Quando o concentrador do acesso emite o pacote da confirmação, pode igualmente prosseguir para a fase de sessão do PPP.

3 Protocolo RADIUS

3.1 Arquitectura AAA

A arquitectura de *Authentication, Authorization* e *Accounting* (em português, autenticação, autorização e contabilização) representa uma parte fundamental do modelo de redes de comunicação actuais e a sua importância irá aumentar à medida que aumentarem o número de utilizadores, os tipos de serviço e a concorrência entre os prestadores de serviço. São as arquitecturas AAA que permitem aos prestadores de serviço a introdução de políticas de acesso, de serviço e de custo.

As arquitecturas de MA encontram-se divididas em três componentes distintos: a autenticação, a autorização e a contabilização dos dados que permitam a quantificação dos recursos usados:

- A autenticação refere-se à implementação de mecanismos que permitam ter a garantia da autenticidade do utilizador que pretende usar o serviço, indispensável para a sua correcta identificação e posterior cobrança dos serviços e recursos por ele usados.
- A autorização refere-se aos mecanismos que permitem ao prestadores de serviço controlar o acesso dos seus utilizadores aos serviços disponibilizados. Actualmente estes mecanismos permitem a coabitação simultânea de vários tipos de serviços, o que possibilita a implementação de políticas diferenciadas, normalmente associadas a diferentes custos.
- Por fim, os mecanismos de AAA definem a forma como é efectuada a contabilização dos dados transferidos que permitem aos prestadores de serviço a cobrança pelos recursos usados pelos respectivos clientes. Nas redes IP tradicionais a informação essencial para a cobrança é o tempo e o volume de tráfego usado pelos clientes. No entanto, a introdução de acessos do tipo *always on* e a possibilidade de mobilidade, obriga a um refinar das formas de contabilização existentes.

3.2 Protocolo RADIUS

O protocolo RADIUS é o protocolo de AAA mais usado nas actuais redes IP. Foi inicialmente desenvolvido a pensar nas ligações de utiliza dores através de acessos telefónicos, vulgo *dial up,* via PPP.

O RADIUS implementa mecanismos de autenticação dos utilizadores, autorização de acesso a serviços e contabilização de informação que permita a facturação do serviço e dos recursos usados pelo cliente. Tem uma arquitectura de cliente - servidor onde as perguntas *(requests,* na terminologia) são sempre iniciadas pelo cliente, o que limita a sua flexibilidade na implementação de serviços. É transportado sobre UDP, pelo que não dispõe de mecanismos de retransmissão em caso de perda de informação, característica que o torna vulnerável em ligações onde a perda de pacotes possa ser significativa.

O mecanismo de funcionamento do RADIUS está representado na Figura 25. As suas entidades principais são o cliente, o ponto de entrada na rede que no caso do *dial-up* é o *Network Access Server* (NAS) e o servidor RADIUS. O servidor RADIUS contém ainda uma base de dados *Lightweight Directory Access Protocol* (LDAP) onde são aguardados todos as informações relativas aos clientes. O utilizador não participa directamente no mecanismo RADIUS.

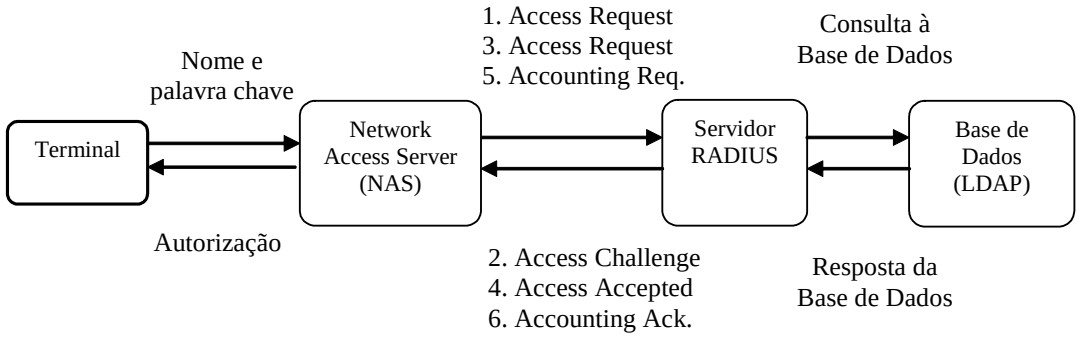

Figura 25 – Protocolo RADIUS

Os procedimentos do mecanismo RADIUS podem ser descritos sumariamente na Figura 52, onde está representado o caso de um cliente que se tenta ligar à rede acedendo através do NAS, indicando-lhe o seu nome de utilizador e palavra chave, via PAP ou CHAP.

Com essa informação, o cliente constrói uma mensagem (#1) *Access Request* que é enviada para o servidor. Após a sua chegada, o servidor consulta a informação referente ao utilizador na sua base de dados. Com base nesta informação o servidor poderá efectuar um desafio ao Cliente em que lhe pede dados adicionais (#2). A resposta ao desafio é dada num novo *Access Request* (#3). Se por fim toda a informação for validada pelo servidor, é dada a autorização para o acesso através de uma mensagem de *Access Accepted* (#4).

Para além dos procedimentos de autenticação, o RADIUS implementa também mecanismos de colecta de dados para tarifação. A colecta de dados é iniciada pelo servidor a pedido do cliente via mensagem de *Accounting Request*. A sua confirmação é dada através de um *Accounting Accepted*. A partir desse momento o servidor RADIUS começa a contagem do tempo de sessão e do volume de dados transferidos. Devido mais uma vez à arquitectura cliente - servidor, os dados de contabilização apenas são enviados do cliente para o servidor após terminada a sessão.

O RADIUS, à parte do seu relevante papel nas actuais redes IP sofre de algumas limitações que fortaleceram o aparecimento de uma nova arquitectura, o DIAMETER. A cabeça das limitações do RADIUS vem a sua reduzida flexibilidade na implementação de serviços. Exemplos destas limitações são a dificuldade de o servidor desligar uma sessão que esteja a decorrer, a impossibilidade de implementação de serviços de contabilização em tempo real dos recursos utilizados (tráfego enviado e recebido) e ainda a não definição de mecanismos de negociação que permitam que os clientes e servidores conheçam as suas capacidades mútuas.

No aspecto da segurança o RADIUS implementa apenas de forma opcional o uso de IPSec (IP Security), o que torna difícil a implementação de associações de segurança entre servidores RADIUS localizados em domínios diferentes, com consequências negativas em situações de *roaming*.

Na Figura 26 apresenta-se um diagrama de mensagens exemplificativo do funcionamento do protocolo RADIUS juntamente com o protocolo CHAP.

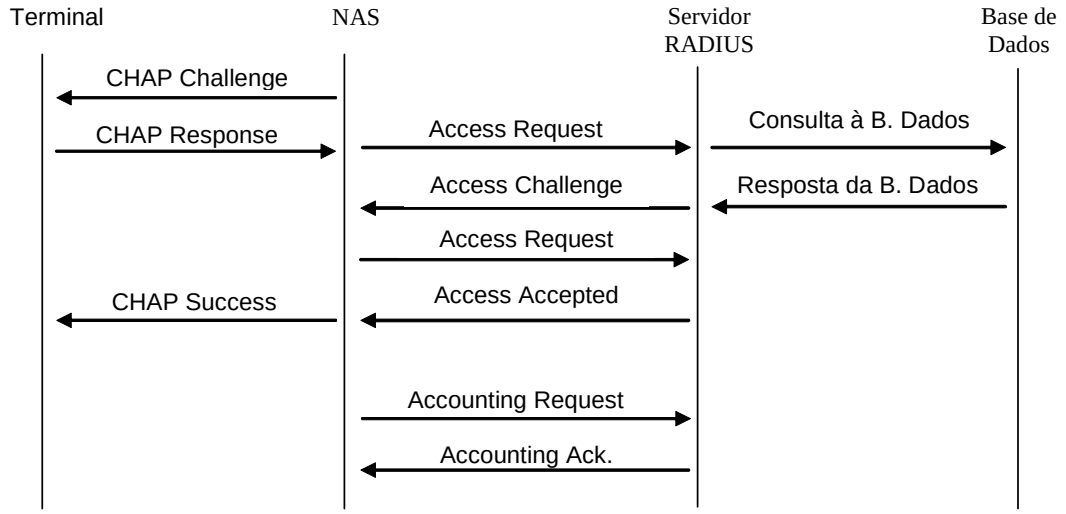

Figura 26 – Diagrama de mensagens do protocolo RADIUS e CHAP

4 Acesso à Internet através de RDIS

O acesso à Internet através da RDIS é uma importante aplicação da RDIS, devido a permitir acessos com débitos bastante mais elevados que os acessos analógicos e com maior qualidade, devido à menor taxa de erros.

O acesso à Internet via RDIS envolve conversão de protocolos de diferentes níveis do modelo OSI, quer nos equipamentos terminais quer nas Gateways entre as duas redes, dependendo das arquitecturas e funcionalidades implementadas, que se analisam em seguida.

4.1 Equipamento terminal de acesso à Internet via RDIS

Os protocolos mais usados actualmente para acesso à Internet via RDIS são o PPP, ML-PPP e V.120, sobre o qual é utilizado o protocolo IP e camadas superiores, TCP ou UDP e aplicações.

No acesso à Internet através de computador pessoal (PC) podemos considerar 4 diferentes arquitecturas, em função do equipamento usado e da localização dos diferentes protocolos.

4.1.1 PC com carta RDIS interna activa

Nesta arquitectura é usada um PC com uma carta de adaptação RDIS activa, isto é, que possui um processador autónomo e *firmware* de implementação de protocolos, nomeadamente PPP ou ML-PPP e sinalização RDIS.

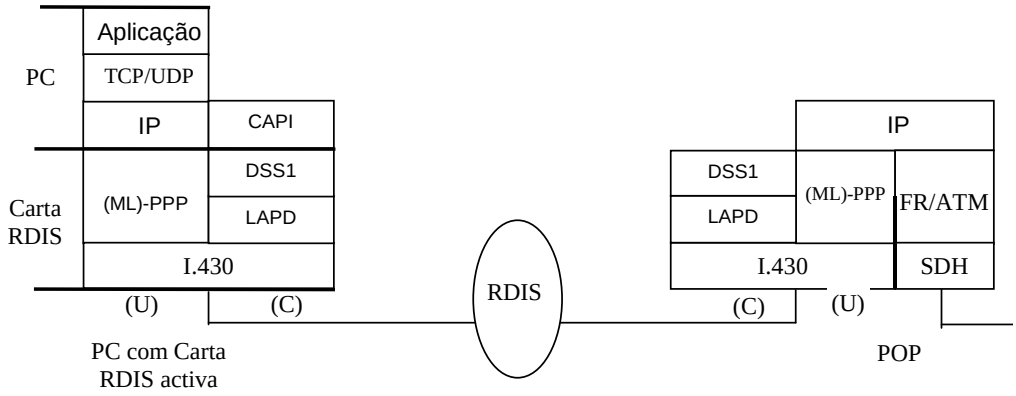

Figura 27 – Diagrama de protocolos de dados de acesso à Internet através de RDIS, canal B

4.1.2 PC com carta RDIS interna passiva

Nesta arquitectura é usada uma carta de adaptação RDIS passiva, sem processador. Neste caso todos os protocolos acima do nível 1(ou parte do nível 2) são implementados pelo PC.

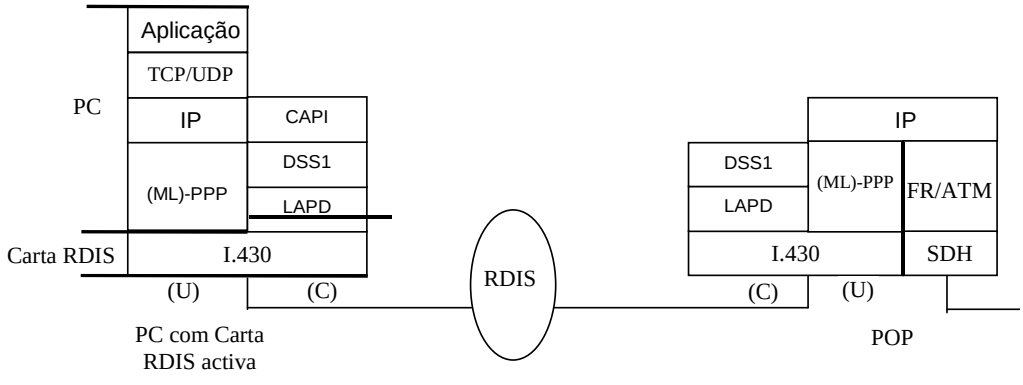

Figura 28 – Diagrama de protocolos de dados de acesso à Internet através de RDIS, canal B

4.1.3 TA RDIS externo

Nesta arquitectura é usado um TA RDIS externo, sendo a interface com o PC feita através de interface RS-232 e Comandos AT. É de salientar neste caso a conversão de PPP ou ML-PPP assíncrono para síncrono no sentido do PC para TA e a conversão inversa no sentido TA para PC.

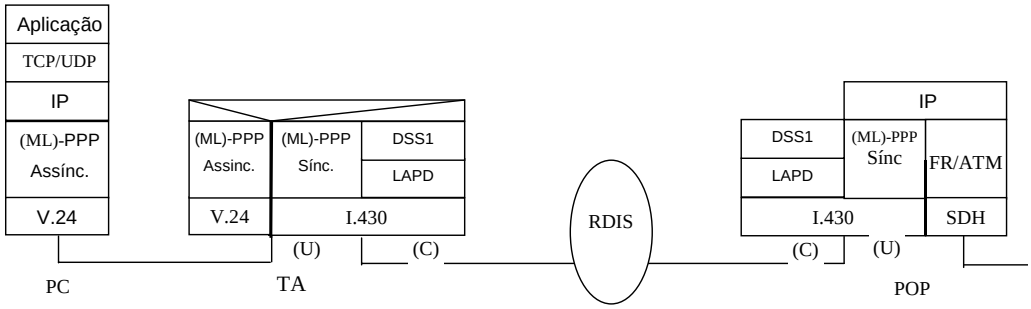

Figura 29 – Diagrama de protocolos de dados de acesso à Internet através de RDIS, canal B

4.1.4 TA RDIS externo com V.120

Nesta arquitectura também é usado um TA RDIS externo, sendo a interface com o PC feita através de interface RS-232 e Comandos AT. A diferença em relação à arquitectura anterior consiste na utilização do protocolo V.120 para transporte de dados entre o TA e o POP.

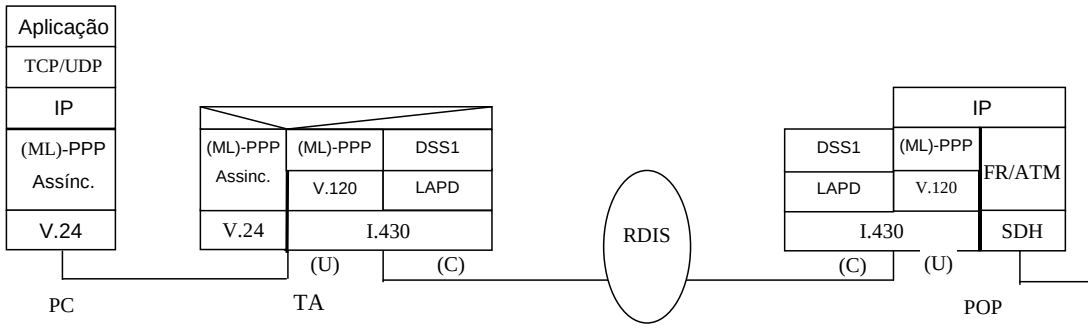

Figura 30 – Diagrama de protocolos de dados de acesso à Internet através de RDIS, canal B

4.2 Diagramas de mensagens de acesso a redes IP

Analisam-se em seguida alguns cenários de utilização da RDIS para acesso a RDIS IP, nomeadamente para acesso à Internet, acesso a LAN e interligação de LANs

Na Figura 31 apresenta-se um exemplo de diagrama de mensagens para o estabelecimento de chamada de acesso à RDIS usando o canal B (Dial-In RDIS)

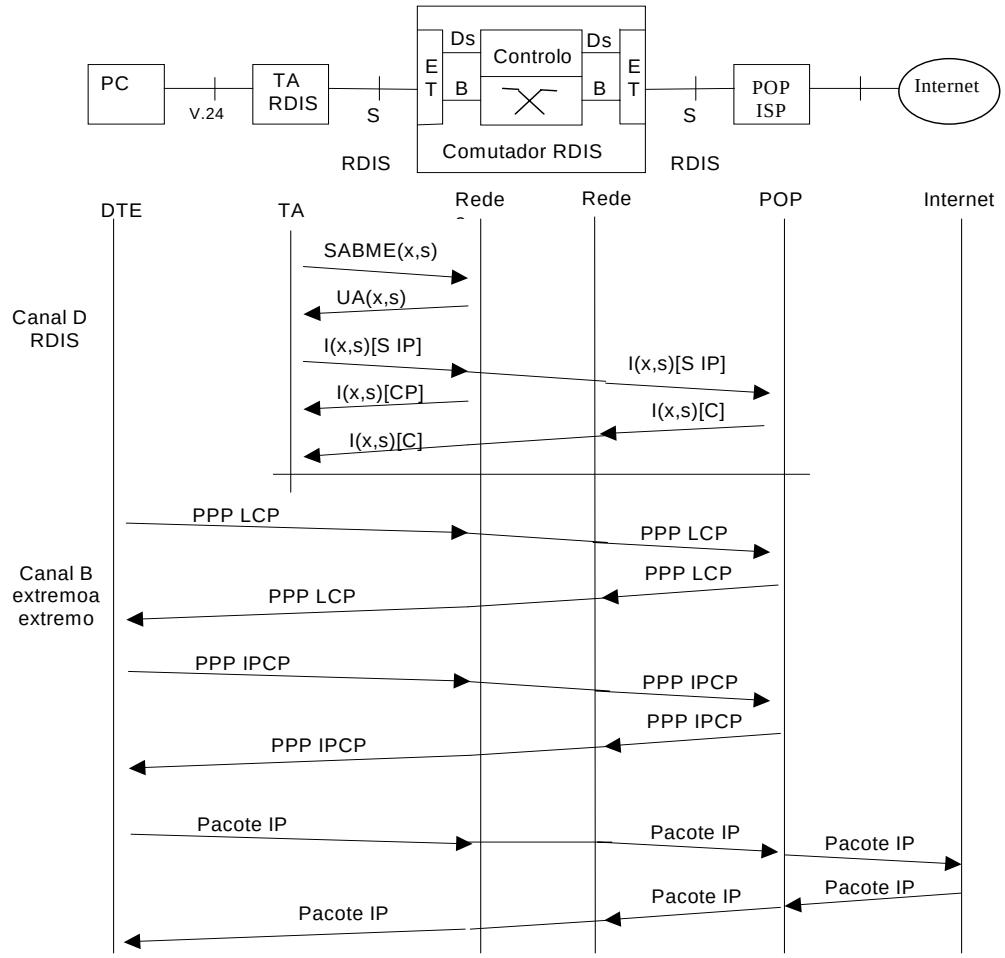

Figura 31 - Estabelecimento de chamada de acesso à Internet no canal B

O acesso remoto a LAN IP é análogo ao do acesso à Internet, pelo que não se representa em detalhe.

Na Figura 32 apresenta-se um exemplo de diagrama de mensagens para o estabelecimento de chamada de interligação de LANs via RDIS usando o canal B.

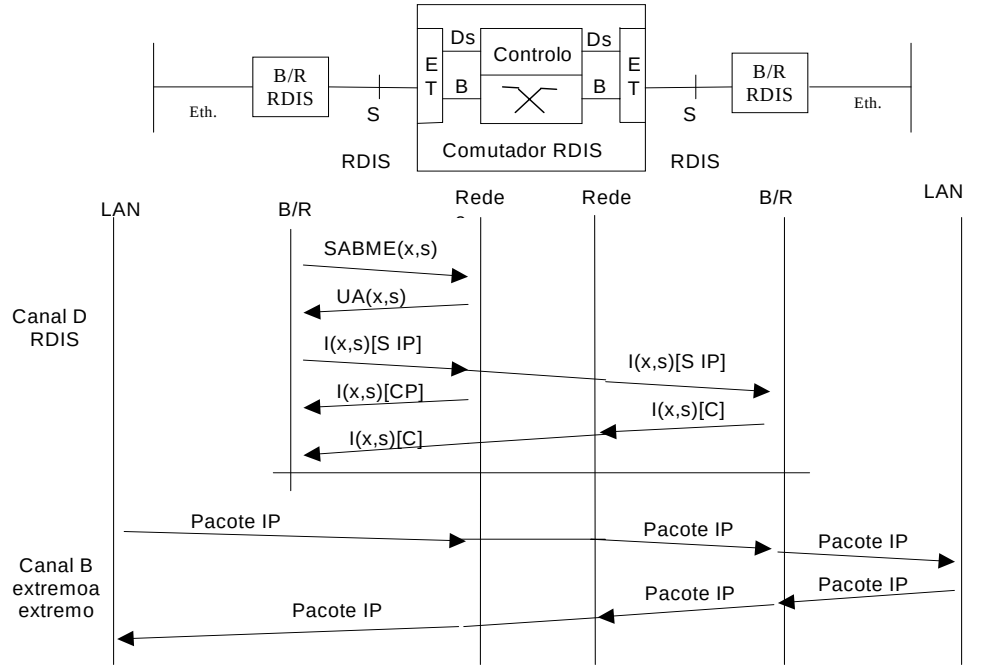

Figura 32 - Estabelecimento de chamada para interligação de LAN com protocolo IP com canal B

4.3 Always On Dynamic ISDN (AODI)

Always On Dynamic ISDN (AODI) é um serviço de rede que proporciona uma conexão sempre disponível, através de uma interface RDIS.

AO/DI é baseado na infraestrutura de centrais digitais RDIS equipadas com comutadores de pacotes X.25 e usando o protocolo BACP (Bandwidth Allocation Control Protocol) definido na RFC 2025. O serviço AO/DI é basedo numa conexão X.25 estabelecida sobre o canal D de RDIS entre o utilizador e o ISP.

O protocolo PPP Multilink e os protocolos TCP/IP são encapsulados no canal lógico transportado no canal D. Os canais B são invocados à medida que é necessária mais largura de banda. Os canais B usam o PPP-ML sem encapsulamento X.25 nem LAPD, isto é usando o canal B transparente até ao POP, sobre o qual são enviados pacotes IP encapsulados em ML-PPP. Na Figura 33 apresenta-se o diagrama de protocolos no acesso à Internet com AO/DI.

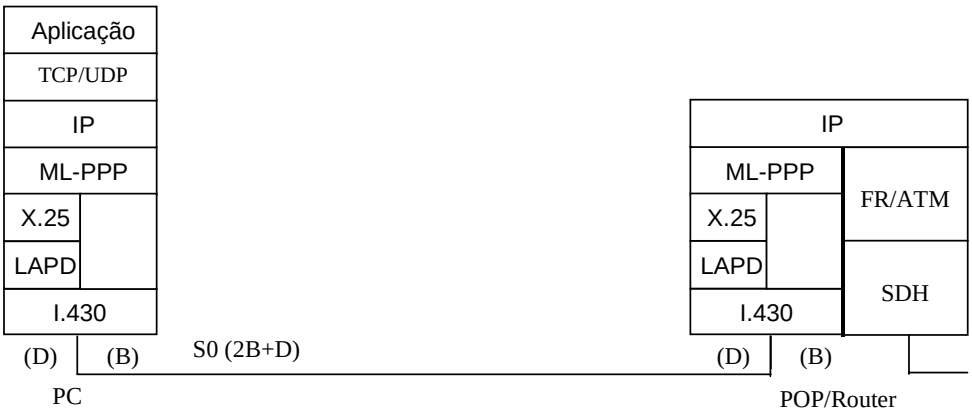

Figura 33 - Diagrama de protocolos no acesso à Internet com AO/DI

É possível fornecer uma ligação full-duplex sempre disponível com base no facto de o nível físico de RDIS puder estar sempre activo, assim como a camada lógica LAPD, o que permite o estabelecimento de um circuito virtual X.25 entre o utilizador e o ISP por onde são enviados os pacotes IP encapsulados em PPP-ML. O facto de as centrais RDIS possuírem comutadores X.25 (*packet handlers*) permite encaminhar os pacotes IP para os Routers do ISP sem atravessar o comutador de circuitos, o que reduz o impacto na rede telefónica.

AO/DI faz uso do protocolo BACP para negociar a largura de banda, gerir a troca de números telefónicos e agregar a banda de conexões posteriores.

Dada a relativamente baixa largura de banda do acesso à Internet no canal D (total de 16 Kbps, com 9600 bps garantido) e o encapsulamento de protocolos, TCP/IP sobre X.25 no canal D tem aplicações limitadas. Há contudo várias aplicações onde a baixa largura de banda sempre disponível é útil, tais como:

- serviços básicos de email
- serviços transaccionais
- teleacção/telecontrolo

Para aumentar a largura de banda para além da disponível no canal D, são usadas mensagens BACP para indicar quando devem ser adicionados canais B ao conjunto de ligações. Os canais B são usados para aumentar a banda disponível num base temporária, sendo desligados quando já não forem necessários.

Com base em estimativas de tráfego são definidas algumas regras que podem ser usadas para pedir largura de banda adicional.

Um canal B é adicionado se o tráfego demorar mais de 5 segundos a transmitir no canal D ou se os dados pendentes forem superiores a 7500 octetos. O estabelecimento, negociação e inicialização de dados do canal B demora na ordem de 3 segundos, correspondente à transmissão de 4500 octetos no canal D. Os receptores AO/DI devem ser capazes de receber dados quer no canal D em X.25 quer nos canais B,contudo na maioria das implementações o emissor deixa de transmitir no canal D enquanto houver canais B activos.

Apresenta-se em seguida um exemplo de heurística para adicionar canais B:

A fila de saída de pacotes está a ficar cheia, isto é, com o débito presente demora mais de 5 seg a esvaziar ? Ou mais de 10 seg ?

- Se o tempo para esvaziar a fila é menor que 5 s use o canal D X.25 sem invocar o canal B.

- Se o tempo para esvaziar a fila é maior que 5 s use o canal D X.25 para enviar um pedido BAP para invocar um canal B.

- Se um canal B estiver disponível use o protocolo PPP-ML para aumentar o débito do serviço,

- Se um canal B não estiver disponível fica à espera que um canal B fique disponível

- Se o tempo para esvaziar a fila é maior que 10 seg, pede 2 canais B.

Após terminar a transferência de dados que requereu a invocação dos canais B adicionais, estes precisam de ser desligados através de pedidos BACP.

Apresenta-se em seguida um exemplo de heurística para reduzir a largura de banda:

- Se não for detectada actividade durante 5 seg, os canais deverão ser desligados.

- Se for detectada uma chamada de entrada através de mensagens DSS1, um canal B deve ser desligado.

- Se for detectada uma chamada de saída através de mensagens DSS1, um canal B deve ser desligado.

Referências

RFC 1661, “The Point-to-Point Protocol (PPP)”, July 1994.

RFC 1570. “PPP LCP Extensions”, January 1994.

RFC 1662, “PPP in HDLC-like Framing”, July 1994.

RFC 1618, “PPP over ISDN”, May 1994.

RFC 1962, “CCP - Compression Control Protocol”, June 1996.

RFC 1332, “The PPP Internet Protocol Control Protocol (IPCP)”, May 1992.

RFC 1144, "Compressing TCP/IP Headers for Low-Speed Serial Links", Feb 1990.

RFC 1994, “PPP Challenge Handshake Authentication Protocol (CHAP)”, August 1996.

RFC 1990, “The PPP Multilink Protocol (MP)”, August 1996.

RFC 2125, “The PPP Bandwidth Allocation Protocol (BAP). The PPP Bandwidth Allocation Control Protocol (BACP)”, March 1997.

RFC 1598, "PPP in X.25", March 1994.

RFC 1973, "PPP in Frame Relay", June 1996.

RFC 2364, "PPP over AAL5", July 1998.

RFC 3336, "PPP over AAL2", December 2000.

RFC 2516, "PPP over Ethernet", December 2000.

RFC 1483, "Multiprotocol Interconnect over AAL5", July 1993.

RFC 3153, “PPP Multiplexed”, August 2001.

RFC 1963, “PPP Serial Data Transport Protocol (SDTP)”, August 1996.

RFC 1989, “PPP Link Quality Monitoring”, August 1996.

RFC 2509, “IP Header Compression over PPP”, February 1999.

RFC 2615, ”PPP over SONET/SDH”, June 1999.

RFC 2661, “Layer Two Tunneling Protocol 'L2TP' “, August 1999.

RFC 2701, “Multi-link Multi-node PPP Bundle Discovery Protocol”, September 1999.

RFC 2823, “PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing”, May 2002.

RFC 2687, “PPP in a Real-time Oriented HDLC-like Framing”, September 1999.

RFC 2138, “Remote Authentication Dial In User Service (RADIUS)”, April 1997

CISCO, Document ID: 42887 (http://www.cisco.com/warp/public/471/ppp_tshoot_gen.html)

Acrónimos

AAL ATM Adaptation Layer
AC Access Concentrator
ACCM Async Control Character Map
ACFC Address and Control Field Compression
ADSL Asymmetric Digital Subscriber Line
AHDLC Asynchronous HDLC
AO/DI Always On Dynamic ISDN
ATM Asynchronous Transfer Mode
BACP Bandwidth Allocation Control Protocol
BAP Bandwidth Allocation Protocol
CHAP Challenge-Handshake-Authentication-Protocol
CID Channel Identifier
CLS Class
CPI Common Part Indicator
CPS Common Part Sublayer
CRC Cyclic Redundancy Check
DCE Data Circuit-terminating Equipment
DNS Domain Name Server
DSS1 Digital Signalling System number 1
FCS Frame Check Sequence
FR Frame Relay
GSM Global System for Mobile
HFC Hybrid Fibre Coax
HDLC High-level Data Link Control
HEC Header Error Control
IANA Internet Assigned Number Authority
IETF Internet Engineering Task Force
IP Internet Protocol
IPCP IP Control Protocol
IPX Internetwork Packet Exchange
ISDN Integrated Services Digital Network
ISP Internet service provider
L2TP Layer Two Tunneling Protocol
LAN Local area Network
LAPB Link Access Procedure, Balanced
LAPD Link Access Procedure for D Channel
LAPDm LAPD for Mobile Links
LAPM Link Access Procedure for Modems
LAPF LAP for Frame Relay
LCP Link Control Protocol
LI Length Indicator
LLC Logical Link Control
LQR Link Quality Report
ML Multi Link
MTP Message Transfer Part
MTU Maximum Transmission Unit.
MRU Maximum Receive Unit
NBNS Netbios Name Server
NCP Network Control Protocol
NLPID Network Layer Protocol Identifier
OSI Open Systems Interconnection
PADI PPPoE Active Discovery Initiation
PADO PPPoE Active Discovery Offer
PADR PPPoE Active Discovery Request
PADS PPPoE Active Discovery Session-confirmation

PAP Password-Authentication-Protocol
PC Personal Computer
PDU Protocol Data Unit
PID Protocol Identifier
POP Point of Presence
PPP Point-to-Point Protocol
PSTN Public Switched Telephone Network
RADIUS Remote Authentication Dial In User Service
RDIS Rede Digital com Integração de Serviços
RFC Request for Comments
SSSAR Service Specific Segmentation and Reassembly
SDH Synchronous Digital Hierarchy
SDL Simple Data Link
SDLC Synchronous Data Link Control
SONET Synchronous Optical Network
SDTP Serial Data Transport Protocol
SNA Systems Network Architecture
SS7 Signalling System number 7
TA Terminal Adaptor
TCP Transfer Control Protocol
UDP User Datagram Protocol
UU User-User Information
UUI User-to-User Indication